

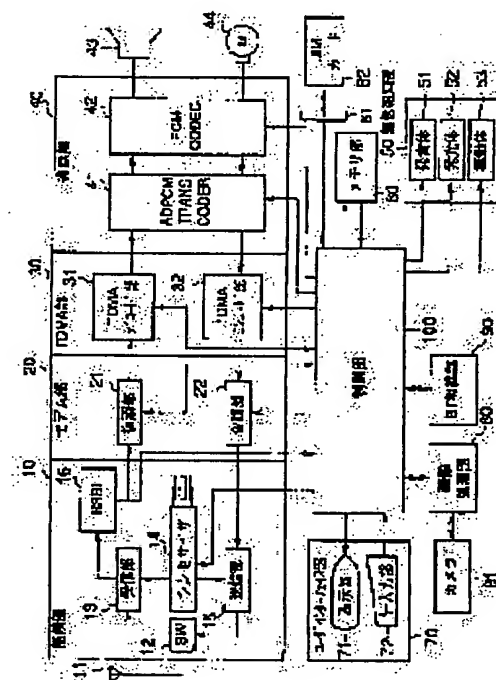
(11)Publication number : 2001-345925
(43)Date of publication of application : 14.12.2001

(21)Application number : 2000-163790
(22)Date of filing : 31.05.2000

(54) MOBILE RADIO TERMINAL

PROBLEM TO BE SOLVED: To provide a mobile radio terminal which can be prevented from being abused by a third person through a connecting interface for connecting external equipment.

SOLUTION: When a utilization limit request such as dial lock is made through a key input part 72, a control part 100 limits utilization of a BT radio part 90, based on conditions corresponding to the request. Once this utilization limit is set, as long as authentication information to be inputted through a camera 81 does not match with authentication information previously stored in a memory part 60, Blue tooth communication using the BT radio part 90 cannot be performed.



[Date of request for examination]

20.04.2007

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(11)特許出願公開番号

特開2001-345925

(P2001-345925A)

(43)公開日 平成13年12月14日(2001.12.14)

(51) IntCl.⁷

識別記号

FI

テーマコート* (参考)

H0 4M 1/673

H O 4 M 1/673

5 K 0 2 7

H04Q 7/38

H O 4 B 7/26

109R 5K067

審査請求 未請求 請求項の数4 OL (全 8 頁)

(21)出題番号

特願2000-163790(P2000-163790)

(22) 出題日

平成12年5月31日(2000.5.31)

(71)出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72)発明者 増田 厚

東京都日野市旭が丘3丁目1番地の1 株
 式会社東芝日野工場内

(74) 代理人 100058479

弁理士 鈴江 武彦 (外6名)

Fターム(参考) 5K027 AA11 BB09 HH11 HH14 HH24
HH26

5K067 AA32 BB04 EE03 EE10 EE35

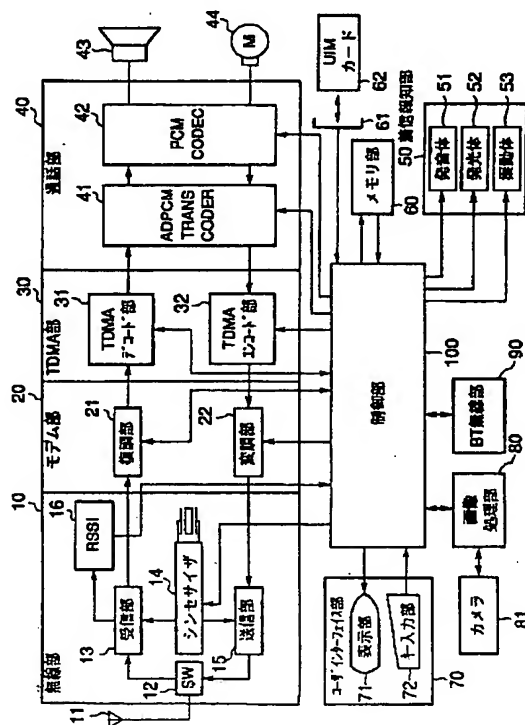
FF02 HH12 HH22 HH23 KK15

(54) 【発明の名称】 移動無線端末

(57) 【要約】

【課題】 外部機器を接続する接続インターフェイスを通じた第三者による悪用を防止可能な移動無線端末を提供する。

【解決手段】 制御部１００は、キー入力部７２を通じて、ダイヤルロックなどの利用制限要求があると、要求に応じた条件に基づくＢＴ無線部９０の利用制限を実施し、一旦この利用制限設定がなされると、カメラ８１を通じて入力される認証情報と、メモリ部６０に予め記憶される認証情報とが一致しない限り、ＢＴ無線部９０を用いたBlue tooth通信は行えないようにしたものである。



【特許請求の範囲】

【請求項 1】 基地局と無線通信する第 1 の通信手段と、前記基地局以外の機器と通信する第 2 の通信手段とを備える移動無線端末において、

予め認証情報を記憶する認証情報記憶手段と、

認証情報を入力する認証情報入力手段と、

制限要求に応じて前記第 2 の通信手段の利用を制限し、

以後、前記認証情報入力手段より入力された情報が、前記認証情報記憶手段に記憶される認証情報と一致する場合に限り、前記第 2 の通信手段を利用可能とする利用制限制御手段とを具備することを特徴とする移動無線端末。

【請求項 2】 前記第 1 の通信手段は、基地局を介して制限要求を受信し、

前記利用制限手段は、前記第 1 の通信手段が制限要求を受信した場合に、前記第 2 の通信手段の利用を制限し、以後、前記認証情報入力手段より入力された情報が、前記認証情報記憶手段に記憶される認証情報と一致する場合に限り、前記第 2 の通信手段を利用可能とすることを特徴とする請求項 1 に記載の移動無線端末。

【請求項 3】 前記第 1 の通信手段が、前記基地局と通信可能であるか否かを判定する通信可否判定手段を備え、

前記利用制限手段は、前記通信可否判定手段の判定結果に基づき、前記第 1 の通信手段が基地局と通信できない場合に、前記第 2 の通信手段の利用を制限することとを特徴とする請求項 2 に記載の移動無線端末。

【請求項 4】 前記認証情報記憶手段は、当該移動無線端末より脱着可能であることを特徴とする請求項 1 乃至請求項 3 のいずれかに記載の移動無線端末。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、例えば携帯電話システムなどの端末装置をはじめとする、外部機器を接続可能な移動無線端末に関する。

【0002】

【従来の技術】従来より携帯電話システムなどの端末装置では、操作部の入力を制限するダイヤルロック機能、メモリ登録したダイヤルのうち正しい暗証番号を入力しないと登録したダイヤルを利用できなくするシークレットダイヤル機能、ダイヤル発信を制限するダイヤル発信制限機能などがあった。また、端末装置の利用制限をサービス網経由で行う方式も考えられていた。

【0003】ところで近時、携帯電話等の端末装置を用いた EC (Electric Commerce) のようなサービスが考えられている。この EC においては、携帯電話システムのネットワークを用いたものの他に、例えば携帯電話の外部インターフェースとして、例えば BT (Blue Tooth) を用いたものも提案されつつある。

【0004】従来の端末装置では、悪意を持つ第三者に

よって、例えばメモリダイヤル情報が読み出されてしまったり、あるいは、EC のように、端末装置の識別情報などを利用して商取引を行う場合には、勝手に端末装置の ID 情報が利用されるなど、端末装置の機能が利用される虞があり、セキュリティ上、大きな問題となり得る。

【0005】

【発明が解決しようとする課題】従来の移動無線端末では、接続インターフェースに接続される外部機器を通じて、例えばメモリダイヤル情報を読み出したり、端末装置の ID 情報を利用するなど、端末装置の機能が利用される虞があり、セキュリティ上問題となっていた。

【0006】この発明は上記の問題を解決すべくなされたもので、外部機器を接続する接続インターフェースを通じた第三者による悪用を防止可能な移動無線端末を提供することを目的とする。

【0007】

【課題を解決するための手段】上記の目的を達成するために、この発明は、ネットワークに接続可能な基地局と無線通信する第 1 の通信手段と、基地局以外の機器と通信する第 2 の通信手段とを備える移動無線端末において、予め認証情報を記憶する認証情報記憶手段と、認証情報を入力する認証情報入力手段と、制限要求に応じて第 2 の通信手段の利用を制限し、以後、認証情報入力手段より入力された情報が、認証情報記憶手段に記憶される認証情報と一致する場合に限り、第 2 の通信手段を利用可能とする利用制限制御手段とを具備して構成するようにした。

【0008】上記構成の移動無線端末では、制限要求に応じて第 2 の通信手段の利用を制限し、認証情報入力手段より入力された情報が、予め認証情報記憶手段に記憶される認証情報と一致する場合に限り、第 2 の通信手段の利用可能とするようにしている。

【0009】したがって、上記構成の移動無線端末によれば、一旦、制限要求を行えば、正しい認証情報が入力されない限り、第 2 の通信手段を利用することができないため、悪意の第三者による第 2 の通信手段の不正利用を防止することができる。

【0010】

【発明の実施の形態】以下、図面を参照して、この発明の一実施形態について説明する。図 1 は、この発明の一実施形態に係わる移動無線端末の構成を示すもので、図示しない基地局との間で、TDMA (Time Division Multiple Access) 方式によって無線通信を行う場合を例に挙げて説明する。

【0011】また、外部機器との接続インターフェースとしては、有線接続によるものと、無線接続によるものが考えられるが、ここでは、BT (Blue Tooth) を用いて無線接続する移動無線端末を例に説明する。

【0012】この図に示す移動無線端末は、アンテナ 1

1を備えた無線部10と、モデム部20と、TDMA部30と、スピーカ43およびマイクロホン44(M)を備えた通話部40と、着信報知部50と、メモリ部60と、インターフェイス61と、ユーザインターフェイス部70と、カメラ81を備えた画像処理部80と、BT無線部90と、制御部100とから構成される。

【0013】移動通信網に接続される基地局から無線通話チャンネルを介して送られた無線周波信号は、アンテナ11で受信されたのち無線部10の高周波スイッチ(SW)12を介して受信部13に入力される。

【0014】この受信部13では、上記受信された無線周波信号が周波数シンセサイザ14から発生された受信局部発振信号とミキシングされて受信中間周波信号に周波数変換される。

【0015】なお、上記周波数シンセサイザ14から発生される局部発振周波数は、無線チャンネル周波数に応じて制御部100より指示される。また、無線部10には受信電界強度検出部(RSSI)16が設けられている。

【0016】この受信電界強度検出部16では基地局から到来した無線周波信号の受信電界強度(以下、RSSIと称する)が検出され、その検出値は制御部100に通知される。

【0017】上記受信部13から出力された受信中間周波信号は、モデム部20の復調部21に入力される。復調部21では上記受信中間周波信号のデジタル復調が行われ、これによりデジタル通話信号が再生される。

【0018】TDMA部30のTDMAデコード部31では、制御部100の指示に従ってタイムスロットごとに上記デジタル通話信号が分解される。そして、この分解された複数のデジタル通話信号のうち、自機宛てのスロットのデジタル通話信号が通話部40に入力される。

【0019】通話部40は、適応差分PCMトランスコーダ(ADPCM TRANS CODER)41とPCMコーデック(PCM CODEC)42とからなり、上記デジタル通話信号はこの適応差分PCMトランスコーダ41およびPCMコーデック42で順次復号されてアナログ通話信号に再生される。そして、このアナログ通話信号は図示しない受話増幅器で増幅されたのちスピーカ43から拡声出力される。

【0020】一方、マイクロホン44に入力された送話音声は、PCMコーデック42および適応差分PCMトランスコーダ41で順次符号化されてデジタル通話信号となり、TDMAエンコード部32に入力される。

【0021】TDMAエンコード部32では、上記適応差分PCMトランスコーダ41から出力されたデジタル通話信号が制御部100から指示されたタイムスロットに挿入されて、変調部22に入力される。変調部22では、

上記デジタル通話信号により搬送波信号がデジタル変調される。このようにして変調された搬送波信号は、送信部15に入力される。

【0022】送信部15では、上記変調された搬送波信号が周波数シンセサイザ14から発生された送信局部発振信号とミキシングされることにより、制御部100より指示された無線チャンネル周波数に周波数変換されたのち、所定の送信電力レベルに増幅される。そして、このようにして送信部15により周波数変換および信号増幅された無線周波信号は、高周波スイッチ12を介してアンテナ11から基地局に向け送信される。

【0023】着信報知部50は、当該端末装置宛てに着信があった場合に、制御部100の制御によりユーザに対して着信を報知するもので、可聴音を発して報知を行なう発音体51と、発光により報知を行なう発光体52と、例えば偏心モータなどにより振動を発生して報知を行なう振動体53とからなる。

【0024】メモリ部60は、例えばROMやRAMなどの半導体メモリを記憶媒体としたもので、この記憶媒体には制御部100の制御プログラムや認証に必要な自機のIDデータ、種々制御データ、各種設定データ、短縮ダイヤル等に対応させたダイヤルデータなどを記憶する他に、所有者を識別するための画像データを認証情報として記憶している。

【0025】インターフェイス61は、UIMカード62を接続するインターフェイスである。UIMカード62は、移動通信システムを運営する事業者との契約情報やユーザの識別情報の他に、公衆網などのネットワークを通じて銀行などから引き出した電子マネーの情報や、電子マネー用の暗証番号を記憶する。

【0026】ユーザインターフェイス部70は、表示部71とキー入力部72とからなる。表示部71は、例えばLCD(Liquid Crystal Display)などからなりユーザに対して自機の状態(発信/着信、バッテリー残量、受信強度)やメモリ部60から読み出したダイヤルデータ、後述するカメラ81にて撮像した画像データなどを視覚的に示すためのものである。

【0027】キー入力部72は、ダイヤル番号入力を行なうためのテンキーなど発信に関わる通常の通話機能を実施するためのキーの他、着信報知方法(可聴音/発光/バイブレータ/報知なし)の切り換えなどの各種設定や種々の機能を利用するためのキーを備えたものである。

【0028】画像処理部80は、CCD又はCMOS固体撮像素子を用いたカメラ81により撮像された画像信号に対し符号化等の画像処理を施して所定の形式の画像データに変換し、制御部100へ入力する。

【0029】BT無線部90は、パーソナルコンピュータやECシステム対応機器との間でBT方式による無線信号の送受信を行う。なお、91は、このBT方式によ

る無線信号を送受信するためのアンテナである。

【0030】制御部100は、例えばマイクロコンピュータを主制御部として備えたもので、上述したようなTDMA方式の通信を行うために通信に係わる各部を制御する他に、キー入力部72を通じたユーザの要求に応じてメモリ部60に記憶されるダイヤルデータの編集制御やカメラ81を用いた画像入力、BT無線部90を通じた通信制御など種々の制御を行う。

【0031】また、制御部100は、UIMカード62に記憶されるデータに基づいて、基地局を通じてネットワーク上の事業者と電子商取引を行うための制御機能や、BT無線部90を通じてECシステム対応機器と商取引を行うための制御機能を備える。

【0032】さらに、制御部100は、新たな制御機能として、メモリ部60に記憶される所有者を識別するための認証情報と、カメラ81を通じて入力される画像データの照合を行い、この照合結果に応じて、BT無線部90を用いた通信機能を制限する制御機能を備える。

【0033】次に、上記構成の移動無線端末の動作について説明する。まず、BT無線部90の利用制限を設定する際の制御動作について説明する。図2は、この制御動作を示すフローチャートで、この処理は、制御部100によってなされる。

【0034】まず、ステップ2aでは、表示部71に認証データを入力するように求める表示を行い、ステップ2bに移行する。ステップ2bでは、画像処理部80を通じてカメラ81を制御する。そして、この制御により、カメラ81にて撮像された画像は、画像処理部80にて画像処理されて、所定の形式の画像データとなり、制御部100に入力され、ステップ2cに移行する。

【0035】ステップ2cでは、ステップ2bにて入力された画像データと、メモリ部60に記憶される認証情報を所定のアルゴリズムで照合し、一致する場合にはステップ2dに移行し、一方、一致しない場合にはステップ2eに移行する。なお、ここで用いられる認証情報は、ユーザの顔などのユーザ固有のものを撮像した画像データを用いる。

【0036】ステップ2dでは、BT無線部90に利用に関わる設定メニュー画面を表示し、ステップ2fに移行する。この設定メニュー画面は、例えば図3に示すような設定項目である。

【0037】この設定項目は、BT無線部90を、常に使用できないように設定する「0：常時OFF」、認証情報を受け付けそれが正しい場合のみ使用可能とする

「1：認証情報照合時ON」、ダイヤルロック時には使用不可能とし、解除時に使用可能とする「2：ダイヤルロック解除時ON」、圏外時などを含む公衆網に接続が行えないような時には使用不可能とし、公衆網に接続が可能時にのみ使用可能とする「3：公衆網接続時」、ダイヤルロックが解除され、なおかつ公衆網に接続が可

能な時にのみ使用可能とする「4：ダイヤルロック解除時+公衆網接続時」、常に使用可能な「5：常時ON」がある。

【0038】ステップ2eでは、入力された認証情報が正しくないものである旨を、表示部71に表示し、ステップ2aに移行して、再度認証情報を入力するように促す。一方、ステップ2fでは、キー入力部72を通じて、ユーザから上記0～5の番号指定を受け付け、この受け付けた番号をメモリ部60に記録し、ステップ2gに移行する。以後、制御部100は、メモリ部60に記録される番号に基づいて、BT無線部90の利用制限制御を実施する。ステップ2gでは、例えば図4に示すように、受け付けた設定番号を表示して、受け付けが完了した旨を表示部71に表示し、当該処理を終了する。

【0039】次に、キー入力部72からの入力を制限するダイヤルロックが設定される場合に、これを解除する際の制御動作について説明する。図5は、この制御動作を示すフローチャートで、この処理は、制御部100によってなされる。

【0040】まず、ステップ5aでは、認証情報の入力を要求する表示を行い、ステップ5aに移行する。ステップ5bでは、画像処理部80を通じてカメラ81を制御する。そして、この制御により、カメラ81にて撮像された画像が、画像処理部80にて画像処理されて、所定の形式の画像データとなり、制御部100に入力され、ステップ5cに移行する。

【0041】ステップ5cでは、ステップ5bにて入力された画像データと、メモリ部60に記憶される認証情報を所定のアルゴリズムで照合し、一致する場合にはステップ5dに移行し、一方、一致しない場合にはステップ5eに移行する。

【0042】ステップ5dでは、入力された認証情報が正しいものである旨を、表示部71に表示し、ステップ5fに移行して、ダイヤルロックを解除し、当該処理を終了する。これ以後、再びダイヤルロックの設定がなされるまで、キー入力部72からの入力は制限されない。

【0043】一方、ステップ5eでは、入力された認証情報が正しくないものである旨を、表示部71に表示し、ステップ5aに移行して、再度認証情報を入力するように促す。

【0044】次に、当該移動無線端末に対して、BT無線部90を利用する要求が与えられた場合の制御動作について説明する。図6は、この制御動作を示すフローチャートで、この処理は、上記要求がなされると、制御部100によって開始される。

【0045】ステップ6aでは、前述の図2に示した処理により、メモリ部60に記録されたBT無線部90の利用制限設定を参照し、この設定で要求される使用制限条件を当該移動無線端末が満たしているか否かを判定する。

【0046】ここで、BT無線部90の利用制限設定に対応する使用制限条件が満たされる場合には、ステップ6bに移行し、一方、満たされない場合にはステップ6cに移行する。

【0047】ステップ6bでは、BT無線部90を制御して、Blue tooth通信を開始するとともに、例えば図7に示すように、表示部71にBlue tooth通信が開始された旨を示す表示を行い、当該処理を終了する。

【0048】一方、ステップ6cでは、例えば図8に示すように、BT無線部90を利用できない（Blue tooth通信は行えない）旨を表示部71に表示し、当該処理を終了する。

【0049】以上のように、上記構成の移動無線端末では、ダイヤルロックなどの利用制限との連動により、BT無線部90の利用制限を容易にでき、一旦、ユーザがBT無線部90の利用制限設定を行うと、ダイヤルロックの解除や正しい認証情報の入力が行われないうり、BT無線部90を用いたBlue tooth通信は行えないようにしている。

【0050】したがって、上記構成の移動無線端末によれば、悪意を持つ第三者が当該端末のBT無線部90を不正に利用しようとしても、ダイヤルロックを解除したり、あるいは正しい認証情報を入力しない限り利用できないため、例えばUIMカード62に記憶される電子マネーを不正に利用したり、あるいはメモリ部60に記憶される種々のデータの不正に読み出したりすることなどを防止することができる。

【0051】尚、この発明は上記実施の形態に限定されるものではない。例えば、上記実施の形態では、認証情報をメモリ部60に記憶させておく構成としたが、これに代わって例えば、認証情報をUIMカード62に記憶させておくようにしてもよい。このような構成によれば、UIMカード62をインターフェイス61に接続しない限り、BT無線部90は利用が制限されることになる。

【0052】また、上述の実施形態では、外部機器を接続する接続インターフェイスとして、BT無線部90を例に挙げて説明したが、これに代わって例えばIrDA（Infrared Data Association）規格に準拠した赤外線通信を行う赤外線通信部や、非同期シリアル通信を行うUART部であっても、同様の効果を奏する。

【0053】さらに、上述の実施形態では、キー入力部72を通じて、BT無線部90の利用制限設定を行うようにしたが、一般の加入者電話や公衆電話機から公衆網および移動通信網を通じて、当該移動無線端末にBT無線部90の利用制限指示を行うようにしてもよい。

【0054】これの具体的な構成としては、図9に示すように、例えば「193+××××××××××（移動無線端末の加入者番号）」のような特番を発呼し、これを受けた移動通信システムの制御局が、当該移動無線端末

に対して、所定の制御情報を含む呼出信号により呼び出しを行う。そして、移動無線端末が呼出信号より上記制御情報を検出すると、BT無線部90の利用制限を実施する。

【0055】このような構成によれば、ユーザが移動無線端末を紛失したり盗まれたりした場合でも、移動通信網を通じた遠隔操作により、悪意の第三者によるBT無線部90の不正利用を防止することができる。

【0056】また、この場合、図2に示したBT無線部90の利用制限処理時に、「3」や「4」のような公衆網に接続が不可能な時を利用制限する設定を行うと、移動無線端末が利用できない圏外などにあると、BT無線部90は利用制限がかけられるため、移動通信網を通じた遠隔操作ができなくても、悪意の第三者によるBT無線部90の不正利用を防止することができる。その他、この発明の要旨を逸脱しない範囲で種々の変形を施しても同様に実施可能であることはいうまでもない。

【0057】

【発明の効果】以上述べたように、この発明では、制限要求に応じて第2の通信手段の利用を制限し、認証情報入力手段より入力された情報が、予め認証情報記憶手段に記憶される認証情報と一致する場合に限り、第2の通信手段の利用可能とするようにしている。

【0058】したがって、この発明によれば、一旦、制限要求を行えば、正しい認証情報が入力されない限り、第2の通信手段を利用することができないため、悪意の第三者による第2の通信手段の不正利用を防止することが可能な移動無線端末を提供できる。

【図面の簡単な説明】

【図1】この発明に係わる移動無線端末の一実施形態の構成を示す回路ブロック図。

【図2】図1に示した移動無線端末のBT無線部の利用制限動作を説明するためのフローチャート。

【図3】BT無線部の利用制限動作の際に、表示部に表示される設定メニュー画面の一例を示す図。

【図4】BT無線部の利用制限動作により利用制限設定がなされた場合に、表示部に表示される設定完了を報知する画面の一例を示す図。

【図5】図1に示した移動無線端末のBT無線部の利用制限の解除動作を説明するためのフローチャート。

【図6】図1に示した移動無線端末のBT無線部の利用要求があった場合の制御動作を説明するためのフローチャート。

【図7】BT無線部を通じた通信が開始された場合の様子を示す図。

【図8】BT無線部を通じた通信が行えなかった場合の様子を示す図。

【図9】移動通信網を通じてBT無線部の利用制限を実施する場合を説明するための図。

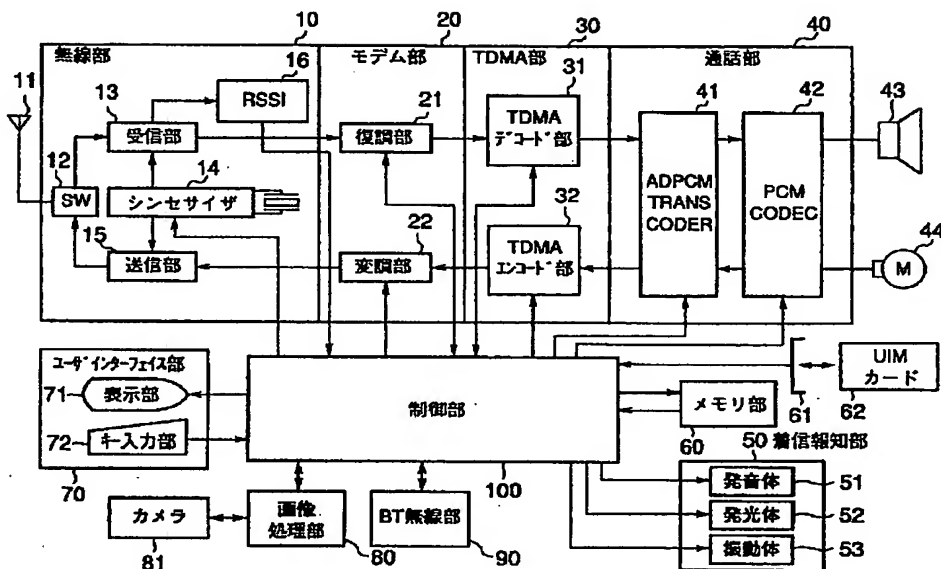
【符号の説明】

10…無線部
 12…高周波スイッチ (SW)
 13…受信部
 14…周波数シンセサイザ
 15…送信部
 16…受信電界強度検出部 (RSSI)
 20…モデム部
 21…復調部
 22…変調部
 30…TDMA部
 31…TDMAデコード部
 32…TDMAエンコード部
 40…通話部
 41…適応差分PCMトランスコーダ
 42…PCMコーデック

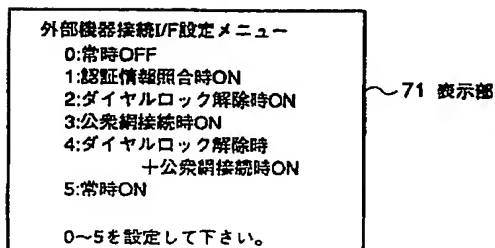
* 50…着信報知部
 51…発音体
 52…発光体
 53…振動体
 60…メモリ部
 61…インターフェイス
 62…UIMカード
 70…ユーザインターフェイス部
 71…表示部
 72…キー入力部
 80…画像処理部
 81…カメラ
 90…BT無線部
 100…制御部

*

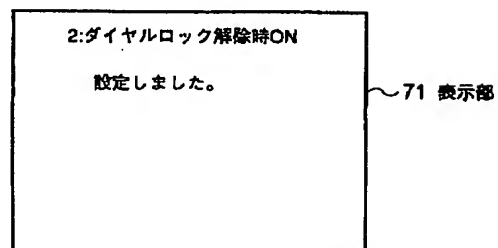
【図1】



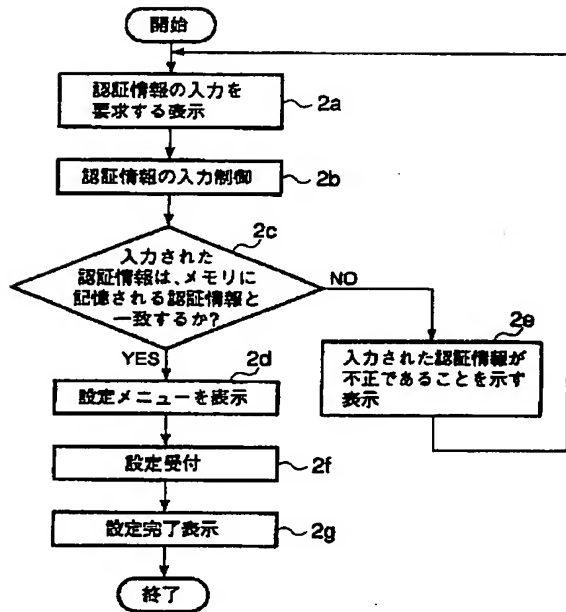
【図3】



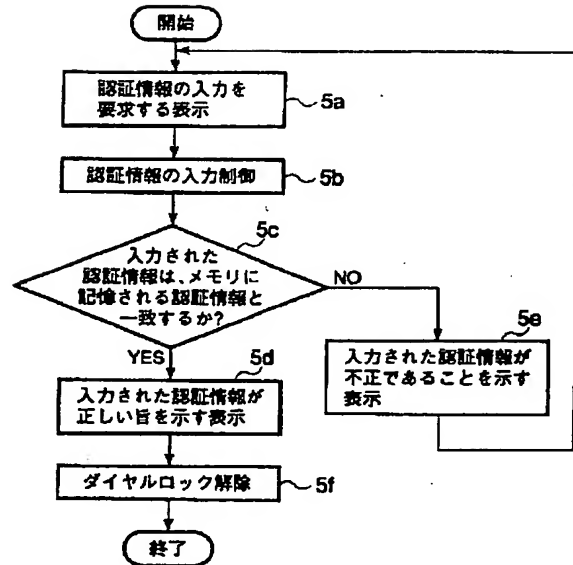
【図4】



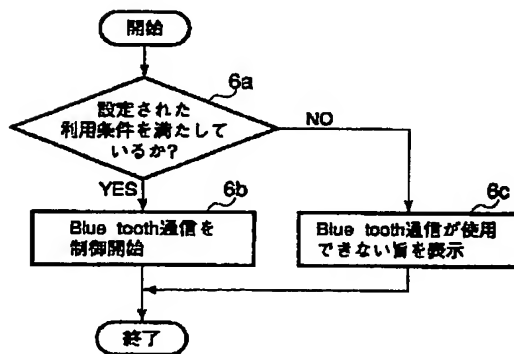
【図2】



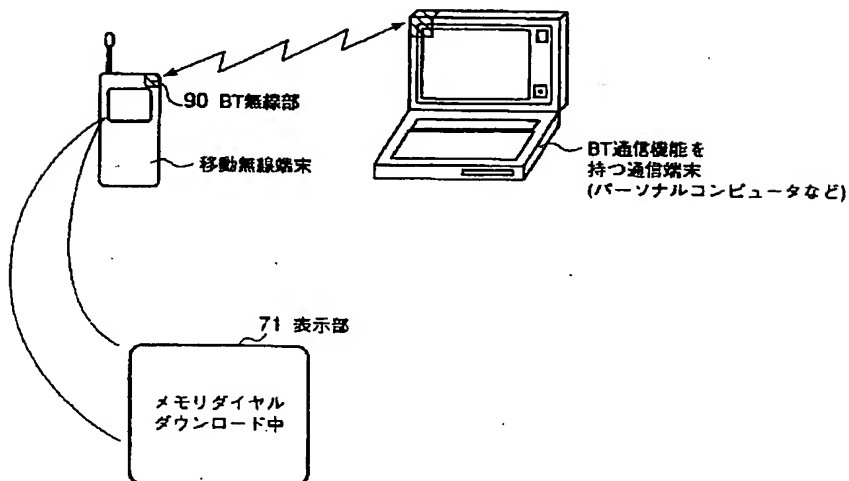
【図5】



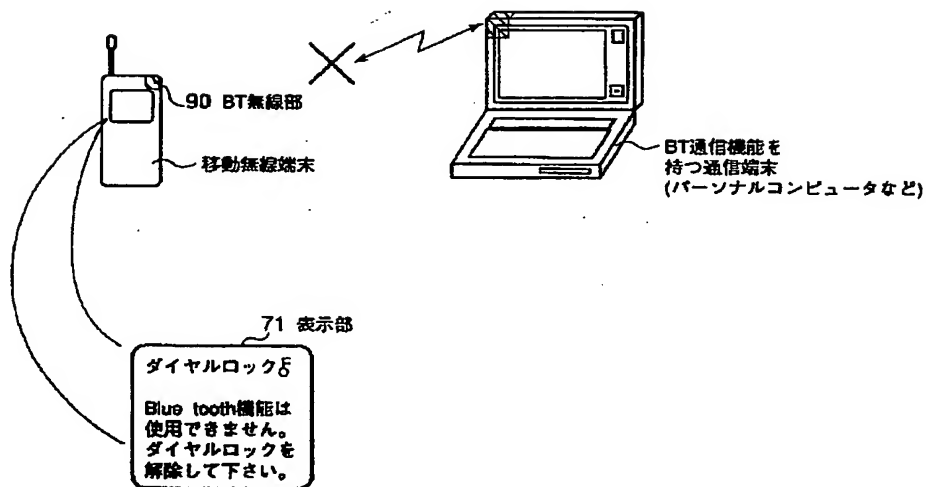
【図6】



【図7】



【図8】



【図9】

